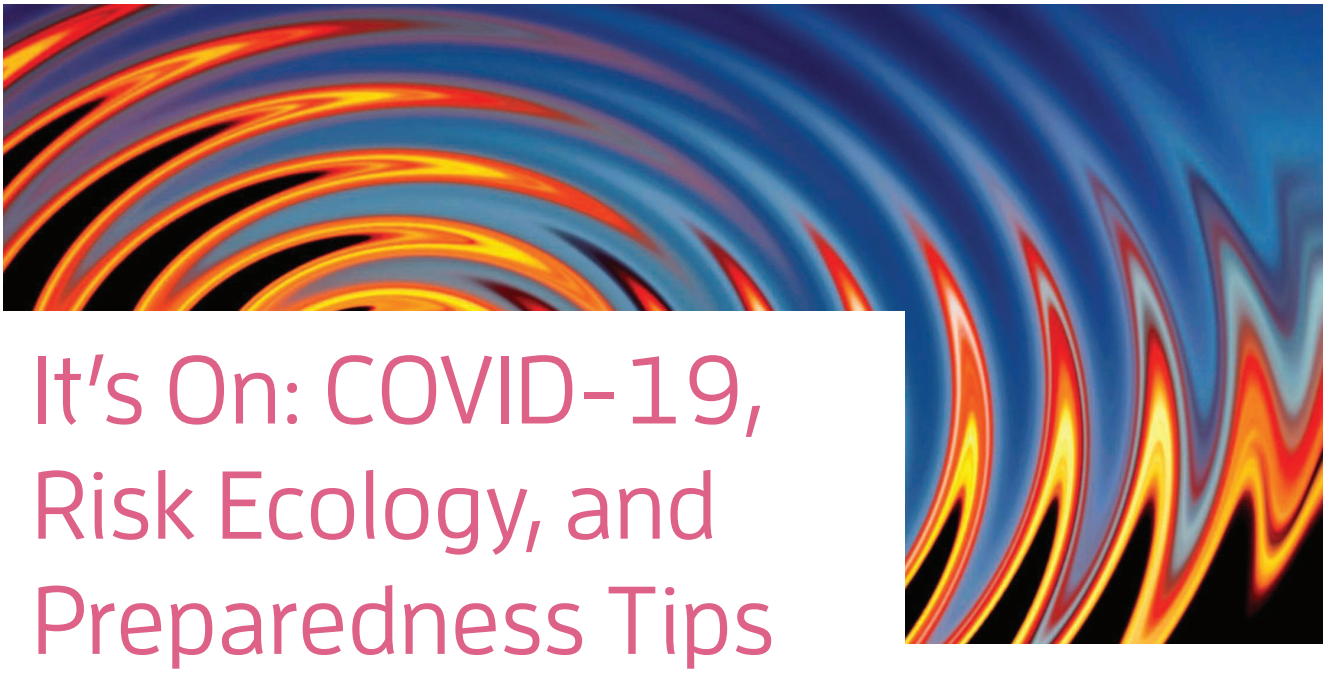


It's On: COVID-19, Risk Ecology, and Preparedness Tips

Hal Berghel, University of Nevada, Las Vegas
Robert N. Charette, ITABHI Corporation
Edward G. Happ and John Leslie King, University of Michigan

"It's on" can mean something big is happening, like the COVID-19 pandemic. In slang terms, it's always on: disruptions are going to happen. This article explores emergency crises, preparedness, risks, surprise, risk fatigue, and tips.

As this issue goes to press, "it's on" can refer to the disruptive COVID-19 pandemic. Millions of people will be infected and hundreds of thousands will die before the pandemic ends. "Social distancing" has entered the lexicon. Companies and agencies have shut down. Economic losses are stratospheric. However, in slang terms, it's always on: disruptions are going to happen, including pandemics, earthquakes, tsunamis, floods, droughts, and wars. Yet, after the fact, people complain that they were unprepared. This article explores emergency crises, preparedness, risks, surprise, risk fatigue, and tips.

The authors have more than a combined 160 years of experience with computing theory, research, design, construction, application, and evaluation. In 1958, March and Simon said scheduled work drives out unscheduled work.[1] Crises drive out everything. Dependence on computerized systems is growing, and the consequences of disruption multiply accordingly. People in computing must do better with what former U.S. Secretary of Defense Donald Rumsfeld called "unknowns," both the known unknowns and the unknowns that often come as a surprise.[2]

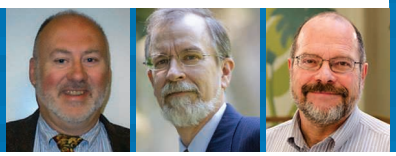
EMERGENCY CRISES AND PREPAREDNESS

An emergency crisis requires a response: determine what is known, assess the resources available, and decide what must be done. Disasters happen all of the time and are becoming more frequent. Annual human-caused crises such as wars, terrorist attacks, or refugee migration peaked at around 250 per year in 2005 and have been declining since (although

Digital Object Identifier 10.1109/MC.2020.2991276
Date of current version: 1 July 2020

 0018-9162/20©2020IEEE

EDITORS
HAL BERGHEL University of Nevada, Las Vegas; hlb@computer.org
ROBERT N. CHARETTE ITABHI Corp.; rncharette@ieee.org
JOHN L. KING University of Michigan; jlking@umich.edu



they might tick up again).[3] Fires and epidemics can be either human or nature caused. Nature-caused crises such as hurricanes, typhoons, winter storms, tsunamis, earthquakes, avalanches, floods, and heat waves produce more monetary damage, sometimes costing billions of dollars, and could accelerate with climate change. Crises vary by onset, from rapid earthquakes to slow droughts, and by duration, from short like a tsunami to long like refugee immigration (see Figure 1). The consequences of crises are growing.

The cost ratio of crisis response to crisis preparedness is about 6:1.[4,5] However, it is difficult to know what investment in preparedness ought to be, given that not all crises have the same priority. It is challenging to predict when or where a crisis will occur or what its consequences will be. In some organizations, a 100-year event is not an executive concern, although it is in others. What is a 100-year event, anyway? The frequency of these incidents might be increasing. The oft-referenced precursor to the COVID-19 pandemic, the so-called Spanish Flu of 1918–1919, was 100 years ago. Crises can damage vulnerable things[6,7] and can make them "old."

Preparedness should be as easy as spotting the intersection of crisis likelihood and cost curves, but implementation can be political. The COVID-19 pandemic has cost the U.S. government more than US$3 trillion so far. At 6:1, preparedness would have cost US$500 billion, nearly the annual U.S. defense budget. This money would probably not have been made available before the pandemic. Crisis preparedness might be popular right after the crisis, but its acceptance fades.

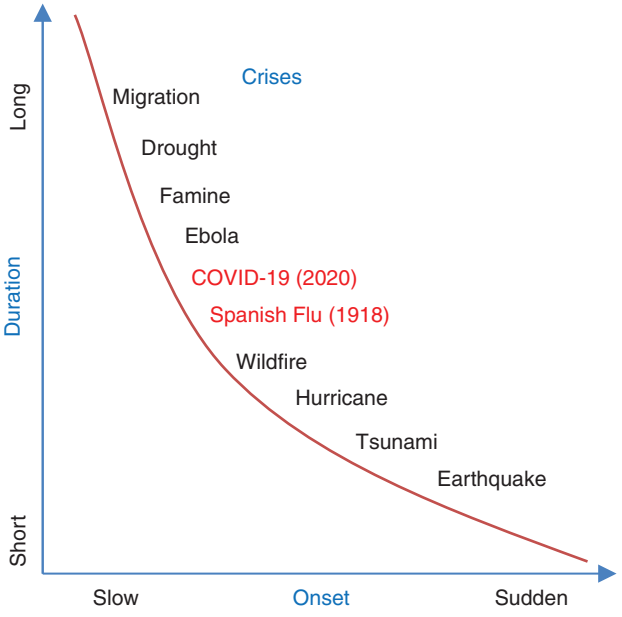


FIGURE 1. The onset versus duration for select natural crises.

There are many unknowns. First responders are 90% locals, often bystanders, and it is impossible to tell in advance who they will be.[8] Hired responders can take too long to get to their destinations. Simple single points of failure might be covered in the backup plan (electricity, telecom, and so on), but staff to execute the plan might not be considered. Planning saves lives. The World Trade Center organizations that lost people on 9/11 had plans, although organizations without plans also lost people. With pandemics like COVID-19, first responders are vulnerable, and even cloud-based systems can be as vulnerable as premised-based ones. There are too many threats to be ready for all of them, but some can be addressed. The best is the enemy of the good: overly ambitious plans fail at run time.

Preparedness means plan and rehearse, including stress testing key infrastructure. However, the definition of infrastructure can be elusive. For example, work infrastructure seldom extends to employees' homes. Staff ordered to work at home become external network customers. Bandwidth to the home is seldom provided like bandwidth to workplaces, and some cannot upgrade. The terrain is changing. Preparedness is difficult, and it may be getting more challenging.

RISK: TURNING WHITE SWANS BLACK

Preparedness requires learning about risk from past experience. The United States has experienced multiple pandemics, including the relatively recent H1N1 and HIV/AIDS cases. Pandemic incidence might be increasing due to global travel, urbanization, human encroachment, environmental exploitation, and the emergence of new infectious diseases (an average of one each year over the past 30 years).[9] Epidemics and pandemics are always "on" in the sense that they are always coming. There may be notable differences, like a greater H1N1 impact among Asian countries or good protection therapeutics for HIV/AIDS. However, incidence was indicated. There would be epidemics and pandemics. Some countries such as Taiwan, Singapore, and Hong Kong have learned from SARS, which influenced fundamental preparedness changes. Others have been slower to learn.

COVID-19, per se, may not have been foreseen, but a pandemic was on. The COVID-19 pandemic started out

as a predictable "white swan" event, although it became a "black swan" with an extreme impact.[10] The public health community warned that a pandemic was inevitable, and the U.S. government has spent billions since 2005 to plan. Congressional hearings and Government Accountability Office reports have explored likelihoods and consequences.[11] Scientific literature projected pandemic infection, morbidity, and mortality, often with recommended steps to reduce risk. The COVID-19 pandemic became a black swan event the same way Hurricane Katrina did in 2005. There were failures at every level, and basic risk principles were violated.[12] The major causes were a lack of information, control, and time, as well as a failure to understand the precedence among them. A lack of information led to a lack of control, which led to a lack of time. Inadequate testing created ignorance of the pandemic's extent and infection dynamics, which thwarted control of the COVID-19 spread. The only tool left was brute-force social distancing, which shut down most of the global economy.

Testing in the United States was slower than in South Korea, Singapore, and Taiwan, all of which did better.[13] The COVID-19 pandemic was underresourced in the United States. Preparedness plans had addressed medical supply needs, but stockpiles were lacking. The priors did not include a major and fast-moving pandemic; it was assumed that no such pandemic would happen. SARS in 2003 and H1N1 in 2009 had modest impacts in most countries, creating complacency in the mistaken view that future pandemics would be mild.

Assumptions are the acceptance of risks. Risks show up at interfaces—interconnections with people, systems, or networks. The more interfaces there are, the more difficult it is to manage risk, and risk-management failures force reliance on powerful but blunt tools like social distancing that might mitigate pandemics but also stop work as interfaces are impaired or cut off. The result is surprise, often called unintended consequences. Surprise is seen in how some U.S. grocers cannot restock their shelves. Interface failure is coupled with dependence on "lean inventory" that keeps minimal on-hand stock in local warehouses. Inventory is in the tightly coupled supply chain discussed later. Interfaces for communicating stocking information to suppliers are built around the assumption that suppliers operate under just-in-time delivery and only when needed. The COVID-19 pandemic crisis has made lean supply chains fragile.

Risk management requires engaging the risk ecology, which is an intersection of business, political, technological, and societal perils. Risk ecology lessons are predicated on interconnectedness as the key to modern systems.

ANY WAR WILL SURPRISE YOU

A reporter once asked U.S. President Dwight Eisenhower about the likely outcome of a crisis. Eisenhower replied, "Any war will surprise you."[14] In a 1906 speech at Stanford University, William James noted that people sometimes try to boost the salience of nonwar problems by making them the "moral equivalent of war." Some have characterized the COVID-19 pandemic as war. This section explains why preparedness can be so difficult. To use another quote from Donald Rumsfeld, "You go to war with the Army you have, not the Army you might wish you have."

First, even simple problems can surprise, as this true account suggests. A computer operations manager at a stock market data center in a New York skyscraper assured superiors of the facility's state-of-the-art fail-over capability, portable generator for electricity, and so on. Then a superstorm hit, and the skyscraper's basement, where the generator, telecom, and electric power circuits were located, filled with 13 ft of salt water. All circuits were fried, and the fault-tolerant computers failed. Everything had to be restored before the market reopened in two days. Crews worked around the clock and got everything back up. Then a worker inadvertently crashed the system. The company missed the market reopening, lost customers, and damaged its brand. To avoid this kind of disaster in the future, the company spent millions of dollars on a roof-top generator and other backups. The lesson was to do this before the disaster. However, a decade later, water in the basement caused two of New York's busiest medical centers to lose power in the wake of Hurricane Sandy.[15] The remediation plans were to prepare to fight the last war, not the next war. Plans did not address the availability of key people, as mentioned earlier.

In a crisis, surprise is revealed by everyday use. One example of this is a variant of the oft-discussed digital divide between haves and have-nots with Internet access that arose when its importance became clear. The COVID-19 pandemic illustrates a divide between "knows" and "know-nots." In 2016, Cambridge Analytica showed the world that a Facebook app, thisisyourdigitallife, was gathering personal information from millions by exploiting weak security and privacy standards as well as layers of epistemic failures.[17–20] The disruptions caused by the COVID-19 pandemic could allow a foothold in commercial media platform news cycles and enable a version of Sarnoff's law, which states that the political value of a message is proportional to the size of the audience and the frequency of the messaging. Crises produce large audiences that are ripe for modern advertising that came of age in the 1918 pandemic to boost morale for the World War I war effort.

Disruptive crises can facilitate controversial practices such as digital surveillance.[25–27] For-profit facial recognition service providers serve law enforcement, governments, and businesses with tools that have few checks on use or vetting for client acceptance.[32] Facial recognition services can match single images to databases of billions of images taken from social

media.[28] Crises like pandemics can fuel image capture while the public is frightened and suspends suspicions. BuzzFeed's assessment of 2,200 clients of facial recognition technology includes authoritarian regimes with questionable human rights records.[34] If COVID-19 draws attention from ethical and legal problems, those issues might become embedded in systems that arise from the pandemic.

COVID-19 might prove to be the opportunity to expand surveillance since organizations take advantage of the alienation and isolation of a population. Payback lies in capturing and monetizing personal information, either disclosed or otherwise. Crises can drive premature action while others are blamed. Some people are motivated by the perception of a threat more than by an actual threat. During crises there may be increased marketing of security systems. Because of the COVID-19 pandemic, ankle bracelet trackers and mobile fences are already in use in some countries. At the same time, there is little news about regulators who monitor behavior that might interfere with the status quo. Companies that promote these new technologies do not always address personal security and privacy issues effectively. Surveillance can backfire by alerting suspects to a location that is under surveillance and may be attacked (target prediction), so something that appears to be risk neutral can have consequences.

However, pandemics can expedite the sharing of data used to track exposure, implement quarantines, and conduct research. An earlier Ebola outbreak caused the U.S. government to relax some of the Health Insurance Portability and Accountability Act requirements to help with sharing, and similar actions have been taken during the COVID-19 pandemic response.[16] Crises can spur innovation by dealing with the unknowns. Ideas that would not have been tried might now be. This is a double-edged sword. Breakthroughs are possible, but foolish mistakes due to inadequate due diligence can be costly and outweigh the benefits. Things can be more difficult than they look. For example, efforts to improve educational infrastructure could now be equivalent to the wet market where COVID-19 made the jump from animals to humans.

Zoombombing shows the pandemic crisis's impact on privacy and security.[21,22] Hard-learned lessons sometimes have to be relearned. There have been periodic pushes for technology in education, such as educational television and computer-assisted education. Halcyon claims such as personalized, self-paced, and self-directed instruction; immediate feedback; asynchronous delivery; and lack of bias have proved to be disappointing. They have not replaced traditional education, proving once again that technology seldom is a panacea.

Breakthroughs are possible, but foolish mistakes due to inadequate due diligence can be costly and outweigh the benefits.

The pandemic has caused education to embrace online classes because there was no other choice. That being said, the net results thus far are not clear. Students and teachers who like online collaboration make it work. The accomplishments of online learning in the COVID-19 pandemic era would not have been possible even 10 years ago. The online comfort level of the students could be a factor, but it is not well understood. The effects of differences in comfort levels among or between students and teachers are theoretically important but unknown. Some like online learning while others do not. Risk assessment is difficult because it is unclear what will or can happen. The risk ecology itself is destabilized, allowing both innovation and mistakes.

This dynamic produces a conundrum for the risk ecology in education. Prior to COVID-19, technology-assisted education, especially online education, was limited to supportive roles despite experiments. In principle, online education is less expensive than the traditional model when the initial development costs can be amortized over a large enough student base (that is, they scale well). The lack of demonstrated educational improvement was offset by efficiency. When online is perceived to save money, it might be used. The COVID-19 pandemic triggered the widespread use of online education because there was no alternative. The verdict awaits. However, there have been a few offers of tuition remission to reflect whatever cost savings institutions realized or the degradation in quality some experienced. Some tuition payers feel they have been charged full price for impoverished service. The conundrum is whether to admit the problems by refunding tuition or forge ahead with online education as mainstream, the "new normal." Aside from the risks involved in contests over tuition remission, important risk issues include reputation and value adds.

The consequences of new business models are sometimes scrutinized less than they should be, especially regarding quality of service and satisfaction of expectations. Serious potential problems can be ignored due to a lack of awareness and understanding. In the case of the push to move to online education, older strategies like interactive, duplex environments (teleconferencing) or rectified or simplex systems (podcasting) might be ignored in favor of more sophisticated services. Such approaches may have been debugged through decades of use, entail minimal expense, and

carry little or no privacy and security risks for participants. However, such suggestions can be met with the response that these capabilities are embedded in commercial platforms. Survival mode can make choices narrow and comparisons difficult. Nevertheless, the allure of sophisticated alternatives is strong, especially when coupled with the loss leader of free service. In fact, free can turn users into exploitable products by exposing them to risk. They have their place as part of a socially responsible, measured, and informed risk ecology. They are not a "go-to" solution.

Dependence is often tied to progress. It is said that necessity is the mother of invention, but invention is also the mother of necessity. People come to depend on inventions. Dependence sneaks up as new circumstances produce cumulative changes over time. Most of the time, things run normally. The desire to make them robust with fault-tolerant design, backups, redundancy, and so on makes them brittle. When disruptions occur, flexibility that maintains the essential is needed. It is not possible to build integrated systems that are simultaneously flexible and robust. During crises, systems must change from robust to flexible, often quickly. With enough complexity, greater flexibility requires controlled disintegration. The automation paradox in cockpits occurs when pilots become dependent on automation for safe aircraft operation, although automation failure requires pilots to know what to do. Sometimes they do not know.

Another example is problems with state unemployment systems that have broken down during the COVID-19 pandemic. One state had massive difficulty in handling unemployment claims, even though it had modernized its system after the Great Recession of 2008–2010. The modernized system was designed to handle only the level of unemployment experienced previously, since the new system requirements assumed unemployment would never be greater than the Great Recession. If the requirements were tied to the Great Depression of the early 1930s, the system would have handled the load. This is another form of preparing to fight the last war.

Finally, there is a link between IT and tightly coupled systems. This article cannot provide a full explanation of these coupled systems, but the attention paid to this topic is likely to increase. Coupling is part of the risk ecology and drives risk. The Allied victory in World War II (WWII) often points to technology like nuclear weapons, code-breaking machines, radar, the Douglas DC-3 planes, the Jeep, antibiotics, and so on. Equally important but discussed less often is how broken-down machines (trucks, tanks, ships, airplanes, and weapons) could be fixed quickly, which is an advantage in mechanized war. These technologies were part of loosely coupled systems and amenable to repair skills learned on farms and in factories served by erratic and often slow supply chains.

After WWII, loosely coupled systems gradually gave way to tighter coupling as knowledge and new technology, especially IT that helped integrate disparate information sources, became more important. Integration produced highly capable systems. A good example is an engine management systems (EMSs) for vehicles with internal-combustion engines. EMSs improved engine performance, fuel economy, and longevity. Without them, meeting progressively stricter emissions standards would not have been possible. However, these tightly coupled systems require specialized know-how, expensive software-controlled diagnostic tools, specialized repair tools, and an elaborate supply chain to be fixed. Few people can repair these engines.

Systems increasingly depend on tightly coupled software. Brooks noted that, with the IBM 360 operating system, fixing tightly coupled systems can introduce new errors.[23] Tightly coupled systems are susceptible to disruptions and difficult to test. During the Cold War, people feared that a Soviet electromagnetic pulse from high-altitude nuclear blasts would cripple tightly coupled U.S. weapon systems while the old-fashioned, loosely coupled Soviet systems remained unharmed. Tightly coupled weapons systems can be difficult or impossible to test without an actual war. Yet tightly coupled systems of all kinds have become ubiquitous and essential. The utility infrastructure increasingly depends on system control and data acquisition (SCADA) networks, often using the Internet. Crucial services, including banking, air travel reservations, unemployment benefits, and other government systems, now operate on systems that are tightly coupled to software developed decades ago.[24] This issue was behind much of the Y2K Problem.

Sociologist Charles Perrow said that tightly coupled systems are prone to "normal accidents."[29] These are not aberrations, and they are inevitable. Tightly coupled supply chains for toilet paper and food have been made famous by the COVID-19 pandemic. Shortages in one supply chain can be offset by surpluses in others. These supply chains were not designed; they evolved. They have never been redirected or stopped, and now they have must be redirected while, in some cases, the pandemic has stopped them. There has been a push to redirect the commercial toilet paper and food supply chains toward residential use. For a time, there were no cargo ships from China in the ports of San Pedro (Los Angeles and Long Beach, California), which are primary Chinese entrepots. As inventory moved from stocks in warehouses to flows aboard "lift," inventory in transit became the *only* form of inventory. As discussed in lean grocery inventory earlier, tightly coupled supply chains cannot be redirected easily. It is not clear what it takes to restart them if they stop. Many unexpected deadly embraces and other problems are likely.

Computerized, tightly coupled systems have become vital to society and the economy. It is increasingly difficult

to predict what failures in such systems might mean. Poor preparedness decisions can carry great risk, with consequences that outlast the crises that prompted them. As noted before regarding privacy and security concerns, social costs can be high. Crises can accelerate already hasty decision processes. When a crisis momentarily provokes attention, the quality of decisions can decline.

RISK FATIGUE

Risk fatigue causes people to turn an ineffective (but not entirely blind) eye to crises, ignoring likelihood or even certainty, dismissing the risk ecology, and preparing to fight the last war. Risk fatigue is normal. While claims that an emergency disruption could not have been foreseen are preposterous in one sense (it's on), they are legitimate in that it is impossible to see the future. An analogous event in recorded history, especially in living memory, proves that such things can happen. Sometimes it is possible to know how frequently they occur and how disruptive they can be. This section discusses the causes of risk fatigue, showing that it is to be expected.

Over time, especially for rare events, the vigilance of individuals and organizations atrophies without recurring triggers (for example, close calls) to heighten awareness.[30] If nothing untoward happens even with triggers, it can take effort and energy to avoid complacency. Constant admonitions by authoritative individuals and organizations to prepare for a crisis wear off as people become comfortable with the notion of the crisis coming. In the case of pandemics, calls for preparation can have the opposite effect by appearing to be overwrought.

Infrequency can cause risk fatigue. Infrequent events, irrespective of intensity, are forgotten. Attention may be paid to emergency preparedness during and immediately after infrequent events, but the people involved disappear and memory fades. Preparation becomes more "real" than the crisis being prepared for. People forget without reinforcement. Strangely, high frequency can also cause risk fatigue as events become routine.

There is also social amplification of risk, in which some risks receive more attention than is called for.[31] The world seems split between infrequent but disruptive events (great tornados, hurricanes, thunderstorms, earthquakes, and so forth, especially in regions where such events seldom occur) and routine events that are handled regularly. Big but infrequent events "never happen" while frequent events are not worth discussing. Any place with frequent huge events is uninhabitable.

Staff designated to be prepared are often involved with IT because, in most organizations, they have experience with systems. Others turn to them to lead preparedness and response. The wireline telephone system was hardened to keep working when other utilities failed. It had its own electrical capability and no end-user data storage. Similarly, large computer systems had uninterruptible power supplies and backup for data storage, while end users had limited local data. As distributed technologies proliferated (cellular telephony, personal computers, and so on), dependency grew as power and data storage exposure increased. IT has become more central, from utility management (namely, SCADA networks) to transaction processing and storage of organizational and personal data. The assurance of robustness falls on IT managers since IT departments have functioned as risk management pioneers in most organizations. The IT department is presumed to have risk expertise.

A particularly problematic task for IT functions is to get others to understand the dynamics of system integration. As noted, risks occur at interfaces that proliferate under system integration. The dream of an integrated system as organizational panacea is old. The Urban Information Systems Inter-Agency Committee (USAC) program ended in 1977, after spending more than US$26 million (more than US$170 million today) to build integrated municipal information systems.[32] Nearly 80 teams of municipalities, computer companies, and universities submitted proposals, and six cities were selected to build integrated systems or subsystems. Ten federal agencies led and paid for USAC. The lead agency was Civil Defense (CD), which was frustrated because cities did not replenish perishable supplies in the Cold War emergency shelters for which CD was responsible. Since integrated, computerized information systems were proposed as the solution to this problem, shelter maintenance became part of routine operational information updates. USAC advanced municipal information systems, but CD's dream was not met. It turned out that integrated systems were not worth the trouble. CD itself eventually fell apart before the end of the Cold War.[33]

TIPS

From the preceding, we provide the following three tips for preparedness.

1. *Pick your battles*: Managing risk is about the future of present decisions. Use "failure imagination" to determine the worst outcome. Manage expectations before and during the crisis. Beforehand, get people to understand that the goal is not to have business as usual during the crisis. Rather, it means prioritization: deciding in advance what will be attended to and what will be ignored. Nobody does more with less. They do less with less. The primary job is to decide what subset of the current will be done and how to transition to that. Policy made during a crisis is temporary. After the crisis, everything returns to the status quo ante bellum. Although lessons learned during the crisis might influence future decisions, there is no replacement for due diligence. A plan to align

authority and responsibility during the crisis is especially important if it is different than normal.

2. *Plan for controlled disintegration*: Systems (technology, supply chains, governance) are becoming more complex and tightly coupled, failures cascade, and failure costs escalate. System integration can make things worse for emergency preparedness. Consider controlled disintegration. Imagine the new, not just the things that everybody knows. For example, during the COVID-19 pandemic, work was often relocated to homes. This might be common in the future or extend to other areas, such as telemedicine. Test for the full capacity needed for such moves. Turn things off to highlight coupling and dependencies. Decide priorities for systems and subsystems in crisis and how they will be maintained. Low-priority items must be decoupled from integrated systems so their problems do not affect essential functions. This must be planned and practiced. Risk is in interfaces. In crises, it must be reduced by becoming less tightly coupled. A firewall must be built against cascading failures by simplifying around crisis essentials. What is important during a crisis may be different from normal. Embrace triage. Recognize that falling over is falling back. Plan how key suppliers, vendors, consultants, utilities, and customers will function in crisis and how to handle those situations.
3. *Test your assumptions*: Assumptions are where 99% of failures start. They are risks taken. Repeatedly and vigorously test assumptions to uncover unknowns and overcome risk fatigue. The risk ecology is always changing as well as assumptions and opportunities to mitigate change. Past risks can fade away while new ones come. The COVID-19 pandemic reveals assumptions that were not tested thoroughly. Soon there will be a surplus of ventilators, yet last year everyone assumed it would take years to produce so many of them.

Multiple cross-cutting threads are presented in this article. Crises are not homogeneous. Some crises impact facilities (for example, fires), others impact people (such as pandemics), while others impact both (in particular, earthquakes). Crises are on—they will happen. There is some evidence that they are becoming more frequent and more complex. There rarely are enough preparedness resources. The key to preparing to function in a crisis with complex systems is to simplify at crisis time, reducing obstacles like privacy and security, knowing that these will be reengaged when the crisis passes. As urgency rises, so does expediency.

REFERENCES

1. J. G. March and H. A. Simon, *Organizations*. New York: Wiley, 1958.
2. D. Rumsfeld, *Known and Unknown: A Memoir*. New York: Penguin, 2010.
3. "Sigma 1/2020: Data driven insurance," Swiss Re Institute, Sigma, Zürich, Switzerland, Feb, 2020, p. 28. [Online]. Available: https://www.swissre.com/institute/research/sigma-research/sigma-2020-01.html
4. L. Lightbody and M. Fuchs, "Every $1 invested in disaster mitigation saves $6: Spending to reduce risk saves lives and creates jobs, key study finds," Pew Charitable Trust, Philadelphia, PA, Jan. 11, 2018. [Online]. Available: https://www.pewtrusts.org/en/research-and-analysis/articles/2018/01/11/every-$1-invested-in-disaster-mitigation-saves-$6
5. "Natural hazards, unnatural disasters: The economics of effective prevention," World Bank and UN, Washington, D.C., 2010, pp. 10, 14. [Online]. Available: http://documents.worldbank.org/curated/en/620631468181478543/pdf/578600PUB0epi2101public10BOX353782B.pdf
6. "ND-Gain Country Index," Notre Dame University Global Adaptation Initiative (ND-GAIN), South Bend, IN, 2017. Accessed on: May 15, 2020. [Online]. Available: https://gain.nd.edu/our-work/country-index/
7. Wikipedia, "List of countries by natural disaster risk," 2017. Accessed on: May 15, 2020. [Online]. Available: https://en.wikipedia.org/wiki/List_of_countries_by_natural_disaster_risk
8. "World First Aid Day: Red Cross Red Crescent calls for expansion of life-saving skills for everyone, everywhere," IFRC, Geneva, Switzerland, Sept. 12, 2014. [Online]. Available: https://www.ifrc.org/en/news-and-media/press-releases/general/world-first-aid-day-red-cross-red-crescent-calls-for-expansion-of-life-saving-skills-for-everyone-everywhere/
9. Institute of Medicine, Forum on Microbial Threats, *Microbial Evolution and Co-Adaptation: A Tribute to the Life and Scientific Legacies of Joshua Lederberg: Workshop Summary (Infectious Disease Emergence: Past, Present, and Future)*. Washington, D.C.: National Academies Press, 2009, p. 5. [Online]. Available: https://www.ncbi.nlm.nih.gov/pubmed/20945572
10. H. R. Morgan, "Why the coronavirus may be a black swan event," Inc., Feb. 29, 2020. [Online]. Available: https://www.inc.com/heather-r-morgan/why-coronavirus-is-a-black-swan-event-we-might-actually-need.html
11. "Lessons from the H1N1 pandemic should be incorporated into future planning," Government Accountability Office, Washington, D.C., GAO-11-632, June 27, 2011. [Online].

Available: https://www.gao.gov/new.items/d11632.pdf
12. R. N. Charette, *Software Engineering Risk Analysis and Management*. New York: McGraw-Hill, 1989. [Online]. Available: https://www.amazon.com/Software-Engineering-Analysis-Management-ENGINEERING/dp/0070106614
13. J. Asquith, "Encouraging Outlook—In Taiwan, Singapore and South Korea life is continuing without lockdowns," *Forbes*, Apr. 1, 2020. [Online]. Available: https://www.forbes.com/sites/jamesasquith/2020/04/01/positive-outlook-in-taiwan-singapore-and-south-korea-life-is-continuing-with-relative-normality/#5b0440eb7335
14. C. Allen, *Eisenhower and the Mass Media: Peace, Prosperity, and Prime-Time TV*. Chapel Hill, NC: Univ. of North Carolina Press, 1993, p. 91.
15. "What caused generators to fail at NYC hospitals?" *CBS News*, Nov. 2, 2012. [Online]. Available: https://www.cbsnews.com/news/what-caused-generators-to-fail-at-nyc-hospitals/
16. J. Davis, "HHS issues limited waiver of HIPAA sanctions due to coronavirus," Health IT Security. [Online]. Available: https://healthitsecurity.com/news/hhs-issues-limited-waiver-of-hipaa-sanctions-due-to-coronavirus
17. C. Wylie, *Mindf*ck: Cambridge Analytica and the Plot to Break America*, New York: Random House, 2019.
18. R. McNamee, *Zucked: Waking up to the Facebook Catastrophe*. Baltimore, MD: Penguin, 2019.
19. K. H. Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President*. London: Oxford Univ. Press, 2018.
20. H. Berghel, "New perspectives on (Anti)Social Media," *Computer*, vol. 53, no. 3, pp. 77–82, Mar., 2020. doi: 10.1109/MC.2019.2958448.
21. A. Zimmerman and C. Veiga, "As NYC bans Zoom for online learning, some schools pause live instruction," Chalkbeat, Apr. 6, 2020. [Online]. Available: https://chalkbeat.org/posts/ny/2020/04/06/nyc-schools-zoom-ban/
22. N. Anderson, "'Zoombombing' disrupts online classes at University of Southern California," *Washington Post*, Mar. 25, 2020. [Online]. Available: https://www.washingtonpost.com/education/2020/03/25/zoombombing-disrupts-online-classes-university-southern-california/
23. F. Brooks, *The Mythical Man-Month*. Reading, MA: Addison-Wesley, 1975.
24. A. Lee, "Wanted urgently: People who know a half century-old computer language so states can process unemployment claims," *CNN*, Apr. 8, 2020. [Online]. Available: https://www.cnn.com/2020/04/08/business/coronavirus-cobol-programmers-new-jersey-trnd/index.html
25. D. Carroll, "Internet worm linked to San Francisco man," *The Harvard Crimson*, Feb. 25, 2009. [Online]. Available: https://www.thecrimson.com/article/2009/2/25/internet-worm-linked-to-san-francisco/
26. O. Thomas, "The person behind a privacy nightmare has a familiar face," *San Francisco Chronicle*, Jan. 22, 2020. [Online]. Available: https://www.sfchronicle.com/business/article/The-person-behind-a-privacy-nightmare-has-a-14993625.php
27. L. O'Brien, "The far-right helped create the world's most powerful facial recognition technology," *Huffington Post*, Apr. 7, 2020. [Online]. Available: https://www.huffpost.com/entry/clearview-ai-facial-recognition-alt-right_n_5e7d028bc5b6cb08a92a5c48
28. R. Mac, C. Haskins, and L. McDonald, "Clearview's facial recognition app has been used by the Justice Department ICE, Macy's, Walmart, and the NBA," BuzzFeed, Feb. 27, 2020. [Online]. Available: https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement
29. C. Perrow, "Normal accident at three Mile Island," *Society*, vol. 18, no. 5, pp. 17–26, 1981. doi: 10.1007/BF02701322.
30. W. R. Freudenburg, "Nothing recedes like success? Risk analysis and the organizational amplification of risks," *Risk, Issues Health Safety*, vol. 3, no. 1, pp. 1–135, 1992.
31. R. E. Kasperson et al., "Social amplification risk: A conceptual framework," *Risk Anal.*, vol. 8, no. 2, pp. 177–187. doi: 10.1111/j.1539-6924.1988.tb01168.x.
32. K. L. Kraemer and J. L. King, "A requiem for USAC," *Policy Anal.*, vol. 5, no. 3, pp. 313–349, 1979.
33. D. Garrison, *Bracing for Armageddon: Why Civil Defense Never Worked*. Oxford, U.K.: Oxford Univ. Press, 1976.
34. C. Haskins, R. Mac, and L. McDonald, "Clearview AI wants to sell its facial recognition software to authoritarian regimes around the world," BuzzFeed, Feb. 5, 2020. Accessed on: May 15, 2020. [Online]. Available: https://www.buzzfeednews.com/article/carolinehaskins1/clearview-ai-facial-recognition-authoritarian-regimes-22?bfsource=relatedmanual

HAL BERGHEL is a Fellow of the IEEE and ACM and a professor of computer science at the University of Nevada, Las Vegas. Contact him at hlb@computer.org.

ROBERT N. CHARETTE is the founder of ITABHI Corporation. Contact him at ncharette@ieee.org.

EDWARD G. HAPP is an executive fellow at the School of Information, University of Michigan. Contact him at ehapp@umich.edu.

JOHN LESLIE KING is a W.W. Bishop collegiate professor at the School of Information, University of Michigan. Contact him at jlking@umich.edu.